L'informatique quantique, une épée de Damoclès pour le chiffrement

A mesure que l'informatique quantique prend peu à peu corps, les experts en sécurité s'inquiètent de ses répercussions sur les technologies actuelles de chiffrement. Car, sur certains calculs en particulier, les qubits – l'équivalent quantique des bits – devraient fournir un tel surcroît de puissance que des technologies aujourd'hui réputées comme sûres seront à la portée d'attaques par force brute.

C'est en tout cas une hypothèse prise très au sérieux par Michele Mosca, le co-fondateur de l'Institut de l'informatique quantique au sein de l'université de Waterloo. Dans un rapport publié par le Global Risk Institute – un organisme financé par des banques et le gouvernement canadien -, le chercheur estime qu'il y a une chance sur sept pour que certaines technologies de chiffrement à clefs publiques actuelles soient cassées dès 2026, en raison de la disponibilité de machines quantiques. Et cette probabilité monte à 50 % à l'horizon 2031. « *Des décisions essentielles doivent être prises* maintenant *afin de répondre demain à ces menaces* », écrit Michele Mosca, qui prêche pour sa chapelle. En effet, le chercheur dirige également un programme de recherche sur les outils de chiffrement capables de résister aux attaques quantiques.

« Nous n'avons plus trop de temps »

Il n'en reste pas moins que la menace que font peser les récentes avancées de l'informatique quantique sur le chiffrement est des plus réelles. Les technologies de codage reposent notamment fréquemment sur la factorisation de grands nombres. Or, en mars dernier, une expérience du MIT et de l'université d'Innsbruck (Autriche) montrait la capacité d'un système quantique composé de seulement 5 qubits à factoriser le nombre 15. Pas encore de quoi faire trembler sur ses bases le chiffrement, mais de quoi donner l'alerte.

« *Aujourd'hui, notre système immunitaire cyber n'est pas prêt à répondre à la menace quantique*, ajoute Michele Mosca. *Nous savons qu'une attaque mortelle [pour les technologies de chiffrement actuelles]plane au-dessus de nos têtes ; et nous n'avons plus trop de temps pour concevoir et déployer le remède avant que cette menace ne se concrétise.* » Pour le chercheur, concevoir des technologies résistant aux assauts des machines quantiques prendra des années, c'est donc aujourd'hui que doit être amorcé l'effort. Selon Michele Mosca, ces systèmes résistant aux capacités de calcul des qubits ne seront pas forcément conçus sur des machines quantiques. Le chercheur explique que des technologies conventionnelles peuvent suffire.

Algorithmes résistant aux qubits

Récemment, Google a pris de premières contre-mesures sur son navigateur Chrome afin de prévenir le décodage des communications chiffrées par des ordinateurs quantiques. De son côté, dans un rapport récent, l'Académie américaine des technologies (le NIST, National Institute of Standard and Technology) estimait que les technologies RSA (par factorisation de nombres

précisément), le chiffrement par courbes elliptiques (ECDSA, ECDH) et le chiffrement DSA ne seront plus sûrs dès qu'un ordinateur quantique verra le jour. Seuls AES et les algorithmes de hachage SHA-2 et SHA-3 devraient échapper au jeu de massacre… mais à la condition expresse de se renforcer. Bref, c'est l'ensemble des technologies de chiffrement et protocoles les implémentant qu'il faudra mettre à jour…

Afin de préparer ce qui s'annonce comme un choc pour la sécurité des échanges électroniques, le NIST entend sélectionner, à des fins de standardisation, au moins un algorithme de chiffrement à clef publique résistant aux assauts des qubits, un autre pour les signatures électroniques et un troisième pour l'échange de clefs. Les candidats devront soumettre leurs propositions en 2017 ; celles-ci seront passées au crible pendant 2 ou 3 ans avant leur standardisation, indique l'organisation. Des sociétés privées ont également pris les devants : le Californien KryptAll a récemment lancé un programme de recherche visant à produire des solutions de chiffrement résistantes aux machines quantiques dès 2021.

A lire aussi :

Un ordinateur quantique casseur de clé de chiffrement

Chiffrement : la machine Enigma de l'ère quantique voit le jour

Un ordinateur quantique chez Google dès 2017 ?

crédit photo © Pavel Ignatov / Shutterstock